# A Preemptive Strike Against An Orwellian Future

Dylan Eleven

Dec 20, 2023 5 min


**ZeroHedge News | Tyler Durden**

**Nick Giambruno | InternationalMan.com**

> ***"If I disappear, make sure this gets out."***

That's what Mark Miller, a young student at Yale, told his closest friends.

**He knew what he was sitting on had revolutionary potential and tha**
**people had disappeared others for much less.**

Miller was steadfast. He wanted to get this information out, even if it was over his dead body.

**In 1977, a group of brilliant researchers at MIT made an astonishing discovery—public-key cryptography.**

It was a mathematical system for encrypting information so that only the intended recipient could read it. It would otherwise take millions of years for the world's most powerful supercomputers to crack.

Cryptography, or the practice of encoding information, is as old as civilization.

One of the oldest known cryptography uses dates back to around 600 BC when the ancient Spartans would pass encrypted messages on thin papyrus sheets. To decrypt the message, the recipient could wrap the papyrus around a scytale (a cylinder of varying dimensions).

The words written on the papyrus itself were gibberish. But you could decrypt the message if you had the right scytale. This is how the Spartans sent and received secret military plans.

**Today, computers allow for radically more sophisticated cryptography.**

That's why the discovery of public-key cryptography was a development of historical significance.

**Never before had unbreakable cryptography been available to the average person. It had always been a government monopoly, and they didn't want to give it up.**

The MIT researchers broke that monopoly in 1977.

The average person could now use public-key cryptography to preserve the privacy of their communications from anyone, including the world's most powerful governments.

Public-key cryptography altered the status quo between the rulers and the ruled. It was similar to the invention of gunpowder or the printing press.

**That's precisely why the US government stopped the publication of this information.**

They threatened the MIT researchers with federal prison if they proceeded under the pretext that the US government considered cryptography a military munition. Those who distributed it would be treated no differently than arms traffickers.

**So, MIT halted plans to distribute the paper… but not before Mark Miller got his hands on it.**

Miller understood the world-changing significance of their discovery. He believed bringing cryptography to the average person was mankind's best chance at avoiding an Orwellian future.

**Miller made countless copies of the MIT research paper at significant personal risk and sent them to his closest friends, prominent computer enthusiasts, magazines, and other media outlets.**

It became clear the cat was out of the bag. The information was already widely available, and there was no point in prohibiting its publication.

**Eventually, the US federal government backed off and allowed the paper to be published.**

It was the spark that would lead to the end of the government's monopoly over cryptography and have profound consequences that nobody could have foreseen.

**The release of public-key cryptography also laid the philosophical and technological foundation for Bitcoin, which would come more than 30 years later.**

But in the meantime, the conflict between cryptography enthusiasts and the government—the Crypto Wars—was just beginning.

# The Crypto Wars

**The US government was not about to throw in the towel so easily.**

While they reluctantly allowed the publication of the MIT research paper on public-key cryptography, they remained opposed to the widespread use of cryptography.

It remained a mostly theoretical discussion for years because there was no practical way to implement public-key cryptography on a mass scale.

**That all changed in the 1990s with the advancement of computers and the Internet.**

**The Crypto Wars were about to heat up again.**

The Clinton administration argued that “Americans have no Constitutional right to choose their own method of encryption.”

They wanted only government-approved cryptography, in which the state would always have backdoor access and the ability to decrypt any message.

The government may have had its way had it not been for the **Cypherpunks**.

The Cypherpunks are a loosely affiliated group of activists advocating for strong cryptography and privacy technologies as a route to social and political change.

They aim to empower the individual and disempower the state, not by engaging in the political process or asking permission, but by writing code and releasing unstoppable software.

The term “Cypherpunk” is derived from “cipher” (a method of encryption) and “punk” (indicative of a counter-cultural ethos).

The movement emerged in the early 1990s as an email list and discussion group.

**A primary concern of theirs was combating the trend of the emerging surveillance state. They believed the widespread use of cryptography was essential to defeat Big Brother.**

In the early 1990s, Cypherpunk Phil Zimmermann released Pretty Good Privacy (PGP), computer software that made public-key encryption available on a mass scale for the first time.

PGP was a direct rebuke of the government's efforts to contain cryptography. The Cypherpunks viewed it as a preemptive strike against an Orwellian future.

The US government was not impressed.

They launched a three-year criminal investigation into Zimmermann because they classified PGP alongside bombs and flamethrowers as a military "munition," a weapon under the purview of government regulation for national security purposes.

The US government sought to charge Zimmermann with violating the Arms Export Control Act, which calls for a penalty of up to 20 years in prison and a $1 million fine.

The US government hoped to make an example of Zimmermann and scare away anyone else from doing the same to prevent cryptography technology from spreading.

But Zimmermann and his Cypherpunk allies didn't back down, even with the prospect of bankruptcy and decades in prison. They understood what was at stake and launched a decisive counterattack.

They printed the PGP code into a book and had it published at a university, knowing that if the government tried to prohibit it, they would likely lose in court.

They even printed the PGP code on a T-shirt to ridicule the government's position.

Eventually, the US government realized it was fighting a losing battle and dropped its criminal investigation of Zimmermann without charging him.

Around the same time, in the *Bernstein v. the US Department of State* case, US federal courts ruled that computer code is equivalent to speech protected by the 1st Amendment of the US Constitution. It set an important precedent and delivered a crucial victory to the Cypherpunks in the Crypto Wars.

**The US government tried to stop the average person from accessing cryptography and failed.**

The Cypherpunks' victory in the Crypto Wars opened the door to many new disruptive technologies—including Bitcoin.

WikiLeaks founder Julian Assange is a Cypherpunk, as are the people behind the Electronic Frontier Foundation, a digital rights advocacy group.

The Cypherpunks were connected with the development of Tor, which stands for "The Onion Router." It encrypts your internet traffic and then hides it by bouncing through a series of computers worldwide to obfuscate your IP address and physical location.

Cypherpunks were also behind BitTorrent, a decentralized, peer-to-peer file-sharing network that is impossible to shut down, unlike centralized services like Napster.

A common theme among the Cypherpunk projects was leveraging cryptography, decentralized networks, and open-source software to create unstoppable technologies.

**However, one thing eluded them… creating a free-market, non-state, digital money.**

**That would eventually come with Bitcoin.**

Today, Bitcoin could be on the cusp of another massive upside explosion.

Historically, Bitcoin's biggest moves to the upside happen very quickly... especially amid a financial crisis.

**With multiple crises unfolding right now, the next big move could happen imminently.**

Original Article: https://www.zerohedge.com/crypto/preemptive-strike-against-orwellian-future